

# Cybersecurity & Data Protection Enhancements for The University of Hong Kong 13 Nov 2024

Eric Moy

CISSP, CISP, CISA, CDPSE, CEH





# Agenda

1. Data Protection
2. Data Privacy
3. AI Security



# Data Protection

- Data Privacy
- Data Security
- Compliance
- Controls



# Data Privacy

- Policies and practices that ensure individuals have control over their personal data, including how it is collected, stored, and used.
- In Hong Kong, this refers to the Six Data Protection Principles (DPP) established by the Office of the Privacy Commissioner for Personal Data.



# Data Security

- Physical Security
- Administrative Controls
- Logical Security



# Physical Security

- Access Control
- Surveillance
- Environmental Controls
- Physical Barriers
- Secure Disposal

# Administrative Control

- Policies and Procedures
- Training and Awareness Programs
- Risk Management
- Incident Response Plans
- Access Review
- Auditing and Monitoring

# Logical Security

- User Authentication (MFA)
- Access Control Lists
- Encryption
- Firewall and Intrusion Detection Systems
- Endpoint protections
- Data Masking and Tokenization
- Security Patches and Updates



# Compliance

- Health Insurance Portability and Accountability Act (HIPPA)
- Payment Card Industry Data Security Standard version (PCI / )  
DSS

# About Security Risk Assessment Audit (SRAA)

Based on 14 domains

- 1. Management Responsibility**
- 2. IT Security Policies**
- 3. Human Resource Security**
- 4. Asset Management**
- 5. Access Control**
- 6. Cryptography**
- 7. Physical and Environmental Security**
- 8. Operations Security**
- 9. Communication Security**
- 10. System Acquisition, Development and Maintenance**
- 11. Out bouncing Security**
- 12. Security Incident Management**
- 13. IT Security Aspects of Business Continuity**
- 14. Compliance**

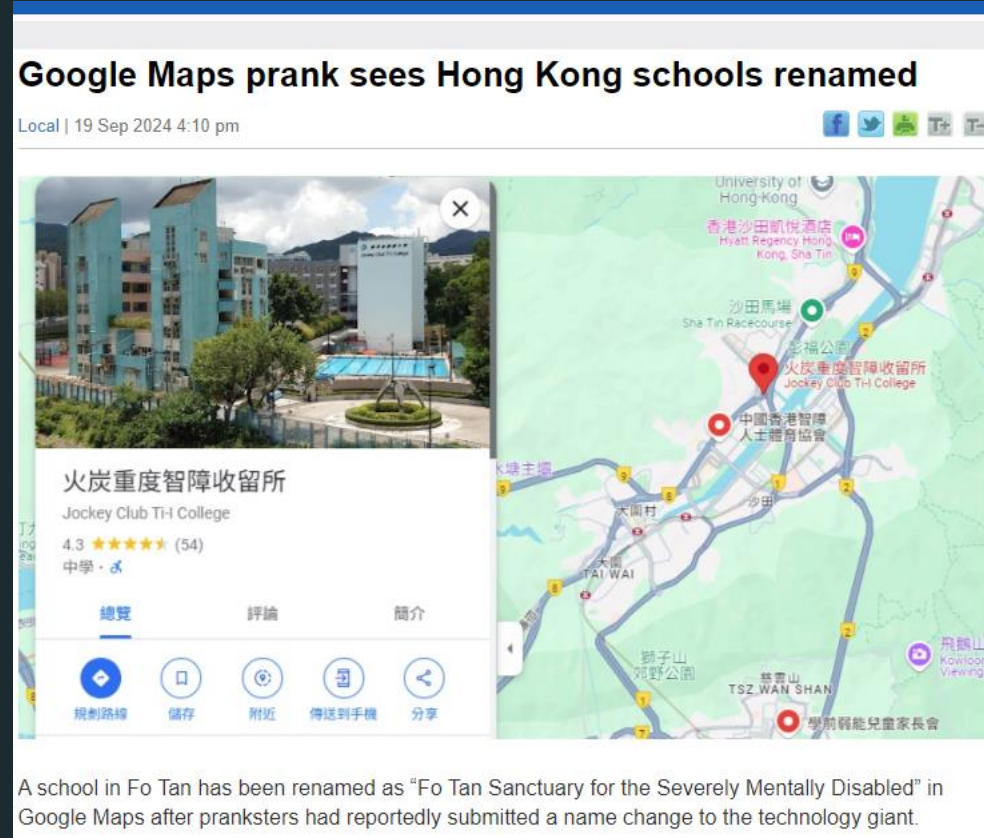


# About Privacy Impact Assessment (PIA)

Based on the Privacy Commissioner for Personal Data

<https://www.pcpd.org.hk/>

# Nothing you can trust



<https://www.thestandard.com.hk/breaking-news/section/4/220659/Google-Maps-prank-sees-Hong-Kong-schools-renamed>

# Quiz Part 1





# Quiz 1.

**Which of the following is considered an element of cyber security?**

- A. Network security**
- B. Operational security**
- C. Application security**
- D. All of the above**

Answer: D

# Quiz 2.

**Malware stands for?**

- A. Multipurpose software**
- B. Malfunctioned software**
- C. Malicious software**
- D. Malfunctioning of security**

Answer: C

## Quiz 3.

**Which of the following is considered as the unsolicited commercial email?**

- A. Virus**
- B. Malware**
- C. Spam**
- D. All of the above**

Answer: C

# Quiz 4.

**What is another name for confidentiality of information?**

- A. Trustworthiness**
- B. Accuracy**
- C. Privacy**
- D. Consistency**

Answer: C

## Quiz 5.

**Which technology removes direct equipment and maintenance costs from the user for data backups?**

- A. An external hard disk**
- B. Network attached storage**
- C. A tape**
- D. A cloud service**

Answer: D



# Data Privacy



# The Privacy Commissioner for Personal Data

<https://www.youtube.com/watch?v=86wYYT8173Q> Chinese

<https://www.youtube.com/watch?v=j6fO6JVGGHg> English

# Basic of Personal Data

## Personal Data

- (1) The information which relates to a **living person** and can be used to identify that person.
- (2) It exists in a form in which access or processing is practicable.



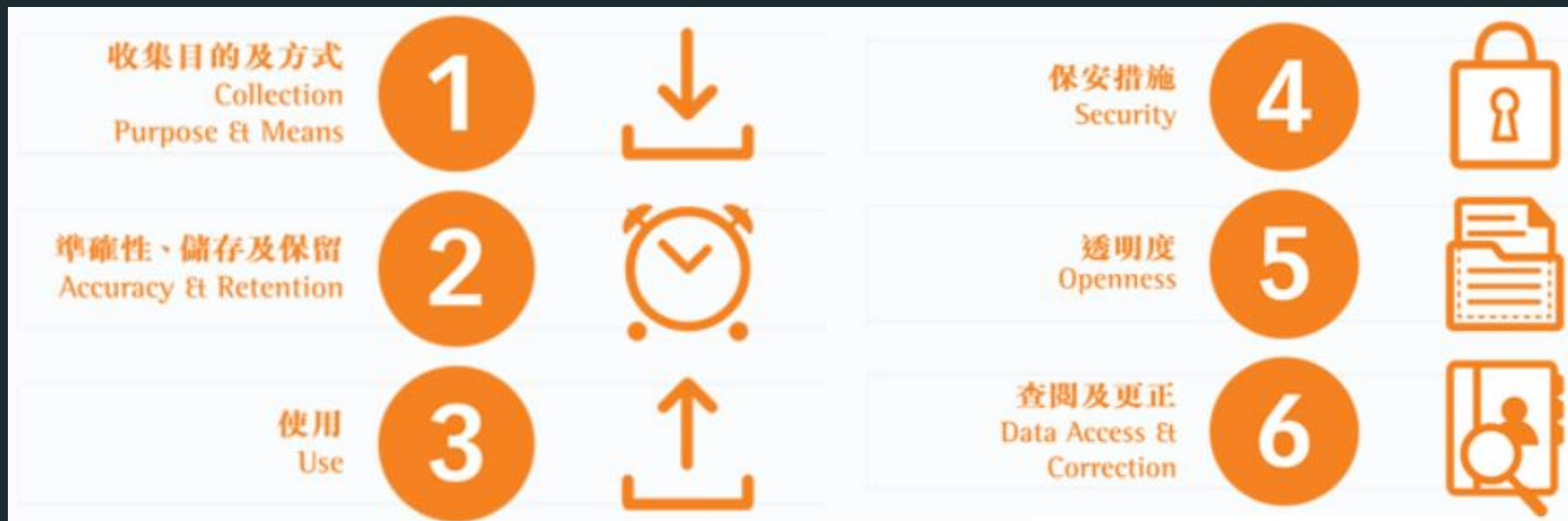
# Basic of Personal Data

## Data User

- A person who, either alone or jointly or in common with other persons, **controls the collection, holding, processing or use of the data.**
- The Data User **is liable** as the principal for the **wrongful act of its authorized data processor.**

# Six Data Protection Principles

Everyone who is responsible for handling data (Data User) should follow the **Six Data Protection Principles ("DPPs")** which represents the core of the Ordinance covering the life cycle of a piece of personal data:





# DPP1 - Data Collection Principle

- Personal data must be collected in a **lawful and fair way**, for a purpose directly related to a function /activity of the data user.
- Data subjects must be notified of the **purpose** and the classes of persons to whom the data may be transferred.
- Data collected **should be necessary but not excessive.**

# DPP2- Accuracy & Retention Principle

- Practicable steps shall be taken to ensure personal data is **accurate and not kept longer than is necessary to fulfil the purpose for which it is used**

# DPP3 - Data Use Principle

- Personal data must be used for the purpose for which the data is collected or **for a directly related purpose, unless voluntary and explicit consent** with a new purpose is obtained from the data subject.

# DPP4 - Data Security Principle

- A data user needs to take practicable steps to safeguard personal data from **unauthorized or accidental access, processing , erasure, loss or use.**

# DPP5 - Openness Principle

- A data user must take practicable steps to **make personal data policies** and practices known to the public regarding the types of personal data it holds and how the data is used.



# DPP6 - Data Access & Correction Principle

- A data subject must be given access to his/her personal data and allowed **to make corrections if it is inaccurate.**

# Privacy Impact Assessment

- The requests are on the rise.



# Privacy Impact Assessment

## Internet Archive hacked, data breach impacts 31 million users

By Lawrence Abrams

October 9, 2024 06:22 PM 35



*Update on 10/20/24 added to the bottom of this article.*

Internet Archive's "The Wayback Machine" has suffered a data breach after a threat actor compromised the website and stole a user authentication database containing 31 million unique records.

<https://www.bleepingcomputer.com/news/security/internet-archive-hacked-data-breach-impacts-31-million-users/>

# Quiz part 2



# Quiz 1.

**What is personal data/PII (Personally Identifiable information)?**

- A. Any data that alone, or in combination with other information, can identify an individual.**
- B. Historical information published about a monument.**
- C. Any information of an employee.**
- D. Information or data that is stored in a vault.**

Answer: A



## Quiz 2.

**What must you do during the collection of a customer's personal information?**

- A. Not collect personal information indiscriminately.**
- B. Not deceive or mislead individuals about the purpose for collecting personal.**
- C. Limit the amount and type of information you collect to what is needed for identified purposes.**
- D. All of the above.**

Answer: D

# Quiz 3.

**Which items come under PII?**

**A.Name**

**B.Email**

**C.Source Code**

**D.All of the above**

Answer: A and B

# Quiz 4.

**When Phishing occurs, is it only done through email?**

**A.Yes**

**B.No**

Answer: B

# Quiz 5.

**How about organizations protect personal information?**

- A. Physical measures, for example, shredding documents and locking desk drawers.**
- B. Organization measures, for example, security clearance and limiting access on “need-to-know” basis.**
- C. Technological measures, for example, the use of passwords and encryption.**
- D. All of the above.**

Answer: D



# Basics of AI and its security implications

# How does AI impact Cyber Security?

- AI has the potential to enhance security, but conversely, it can also be harnessed for malicious purposes, ranging from widescale attacks generation of AI-driven content
- AI-powered cyber attacks use machine learning to analyze a human or machine target and find techniques most likely to help compromise an organization

# Strengths of using AI?

- **Strengths:**

- Enhanced data analysis capabilities
- Improved decision-making
- Multitasking and efficiency
- New skills and expertise
- Objectivity and reduced bias
- Full time availability (24 / 7)
- Reduce human error
- Enhanced efficiency and productivity (e.g. chatbots)
- Increased innovation



# Weaknesses of using AI?

- **Weaknesses:**
  - Overreliance on AI
  - Black box problem
  - Ethical considerations (e.g. data privacy)
  - Job displacement concerns
  - Technical requirement (new key words to learn)
  - Data Leakage while training the AI

# AI Crime

- Phishing
- ID theft
- Deep fakes
- Fake news
- Social engineering
- Chatbot scams

# What is the objectives for the AI Cybercrime?

**Your money**



# AI Robot Kidnapping (Not verified)



<https://www.youtube.com/watch?v=ANByPOXwxQ&t=145s>

# Deep Fakes

**Deep Fakes, which are image, videos, or audio recordings altered using AI. They used in**

- **Disinformation campaigns**
- **Election interference**
- **Blackmail**
- **Bullying**
- **Harassment**
- **Nonconsensual pornography**
- **Hoaxes**
- **Fake news**
- **Financial fraud and scams**

<https://www.security.org/resources/deepfake-statistics/>

# Deep Fakes



[https://www.pcpd.org.hk/english/news\\_events/media\\_statements/press\\_20240801.html](https://www.pcpd.org.hk/english/news_events/media_statements/press_20240801.html)

yahoo! 財經

## 「AI尹光」大受歡迎 能否出道轉化盈利？







**Yahoo 財經**  
 更新日期：2023年6月10日



深度仿冒 (Deepfake) 技術出現的「AI尹光」，獲網民稱讚演繹

繼早前「AI孫燕姿」成為熱話之後，近日有網民製作「AI尹光」，以其獨特唱腔演繹林家謙的

[https://hk.finance.yahoo.com/news/%E3%80%8C%E5%B0%B9%E5%85%89%E3%80%8D%E5%A4%A7%E5%8F%97%E6%AD%A1%E8%BF%8E-%E8%83%BD%E5%90%A6%E5%87%BA%E9%81%93%E8%BD%89%E5%8C%96%E7%9B%88%E5%88%A9%E5%8F%BC%9F-235928322.html?guccounter=1&guce\\_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLnNvbS8&guce\\_referrer\\_sig=AQAAANeJu-X0KY3wOykVxXsoFJtsaw1IHGpX49OzLFRVfwGzYhEi1dOJUth7o5jyFfTwQWgSpSJuxas1A5c\\_0NMEbO5MJzz2qR4RhFzv](https://hk.finance.yahoo.com/news/%E3%80%8C%E5%B0%B9%E5%85%89%E3%80%8D%E5%A4%A7%E5%8F%97%E6%AD%A1%E8%BF%8E-%E8%83%BD%E5%90%A6%E5%87%BA%E9%81%93%E8%BD%89%E5%8C%96%E7%9B%88%E5%88%A9%E5%8F%BC%9F-235928322.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLnNvbS8&guce_referrer_sig=AQAAANeJu-X0KY3wOykVxXsoFJtsaw1IHGpX49OzLFRVfwGzYhEi1dOJUth7o5jyFfTwQWgSpSJuxas1A5c_0NMEbO5MJzz2qR4RhFzv)

# Deep Fakes

[/ ABA Groups](#) / [Center for Public Interest Law](#) / [Standing Committee on Election Law](#) / [Task Force for American Democracy](#) / [Resources](#)

Background >

Problem Statement

Proposed Solution

Next Step

Addendum I

Addendum II

May 06, 2024 ABA TASK FORCE FOR AMERICAN DEMOCRACY

## Deepfakes and American Elections

N. David Bleisch

Share:

[f](#) [t](#) [in](#) [✉](#) [🖨](#)

### Background

Innovation is a double-edged sword. This is poignantly exemplified by the digital phenomenon known as “deepfakes.” Deepfakes are hoax images, sounds, and videos that convincingly depict people saying or doing things that they did not actually say or do. Enabled by generative artificial intelligence and other sophisticated technologies, deepfakes have

[https://www.americanbar.org/groups/public\\_interest/election\\_law/american-democracy/resources/deepfakes-american-elections/](https://www.americanbar.org/groups/public_interest/election_law/american-democracy/resources/deepfakes-american-elections/)



# Deep Fake



Scam<https://news.rthk.hk/rthk/en/component/k2/1739119-20240204.htm>

# Deep Fake



# Online Job Scam

*Crime in Hong Kong* *Hong Kong / Law and Crime*


## 81 Hongkongers swindled out of HK\$12 million in online job scams in past week

One victim duped out of more than HK\$400,000 in click farming job scam after receiving WhatsApp message, police say

Reading Time: **2 minutes**

Why you can trust SCMP 



Listen 

[https://www.scmp.com/news/hong-kong/law-and-crime/article/3282252/81-hongkongers-swindled-out-hk12-million-online-job-scams?module=top\\_story&pgtype=section](https://www.scmp.com/news/hong-kong/law-and-crime/article/3282252/81-hongkongers-swindled-out-hk12-million-online-job-scams?module=top_story&pgtype=section)

# Online Job Scam

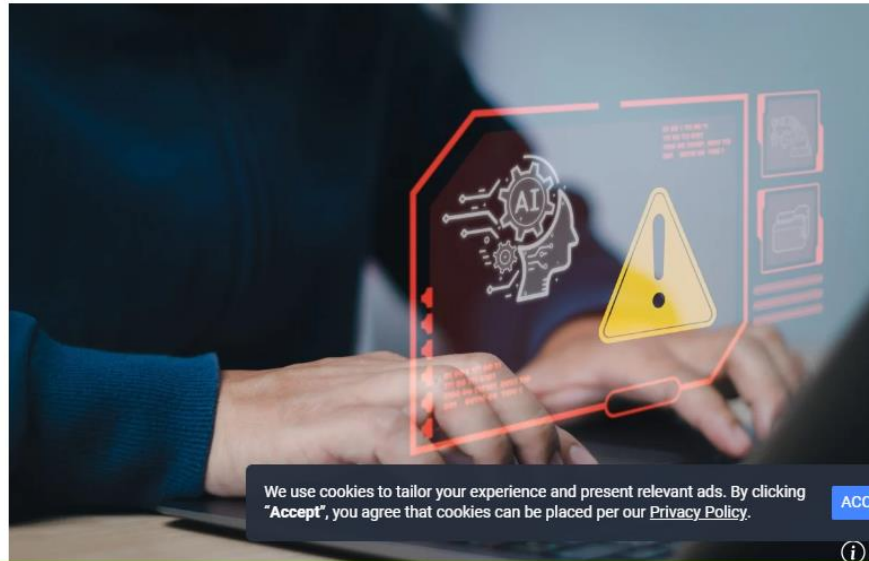
## Hong Kong fraudsters use deepfake tech to swindle love-struck men out of HK\$360 million



Victims included men from Hong Kong, mainland China, Taiwan, India and Singapore, police say

Reading Time: 3 minutes

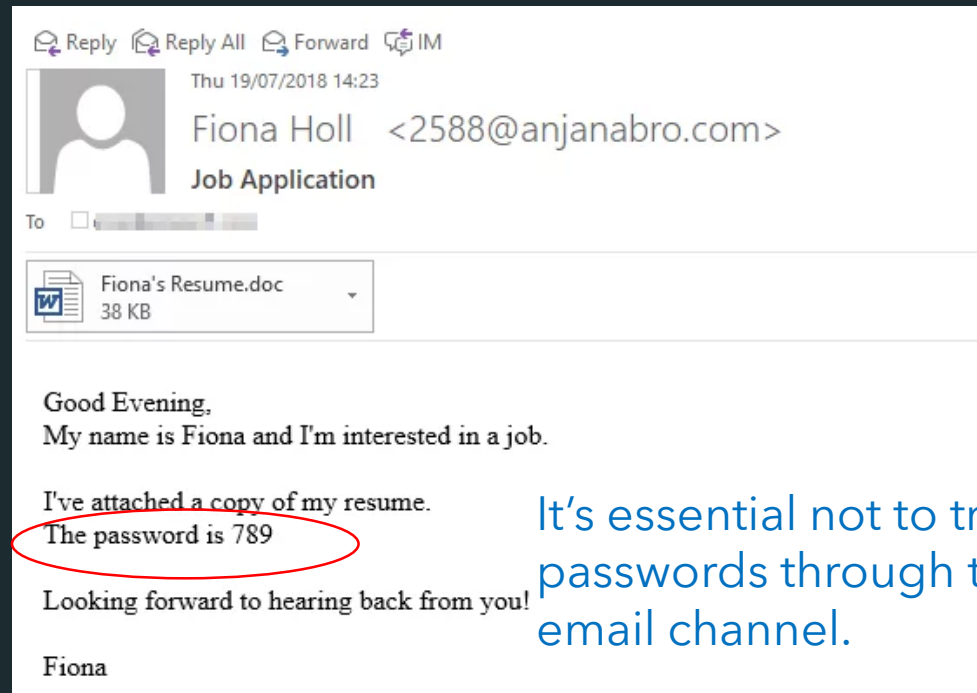
Why you can trust SCMP



[https://www.scmp.com/news/hong-kong/law-and-crime/article/3282345/hong-kong-fraudsters-use-deepfake-tech-swindle-love-struck-men-out-hk360-million?module=top\\_story&pgtype=homepage](https://www.scmp.com/news/hong-kong/law-and-crime/article/3282345/hong-kong-fraudsters-use-deepfake-tech-swindle-love-struck-men-out-hk360-million?module=top_story&pgtype=homepage)

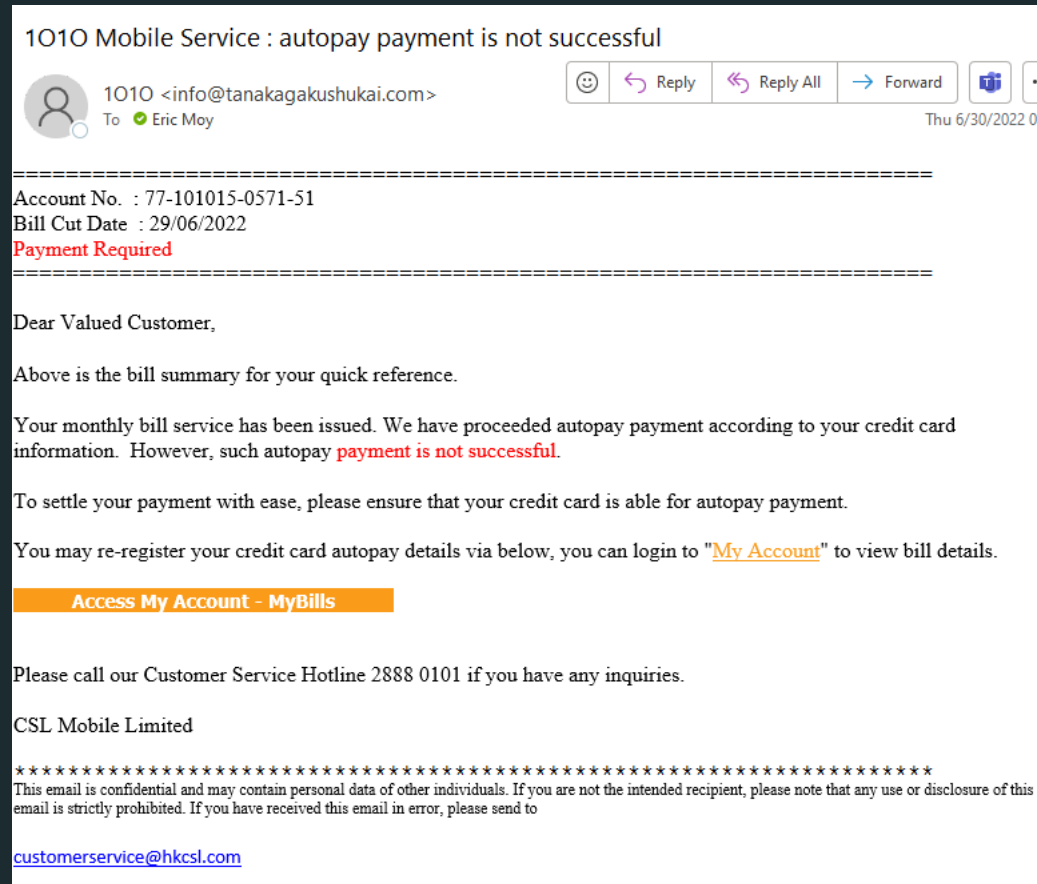
# Phishing example

- What is wrong with the following email?

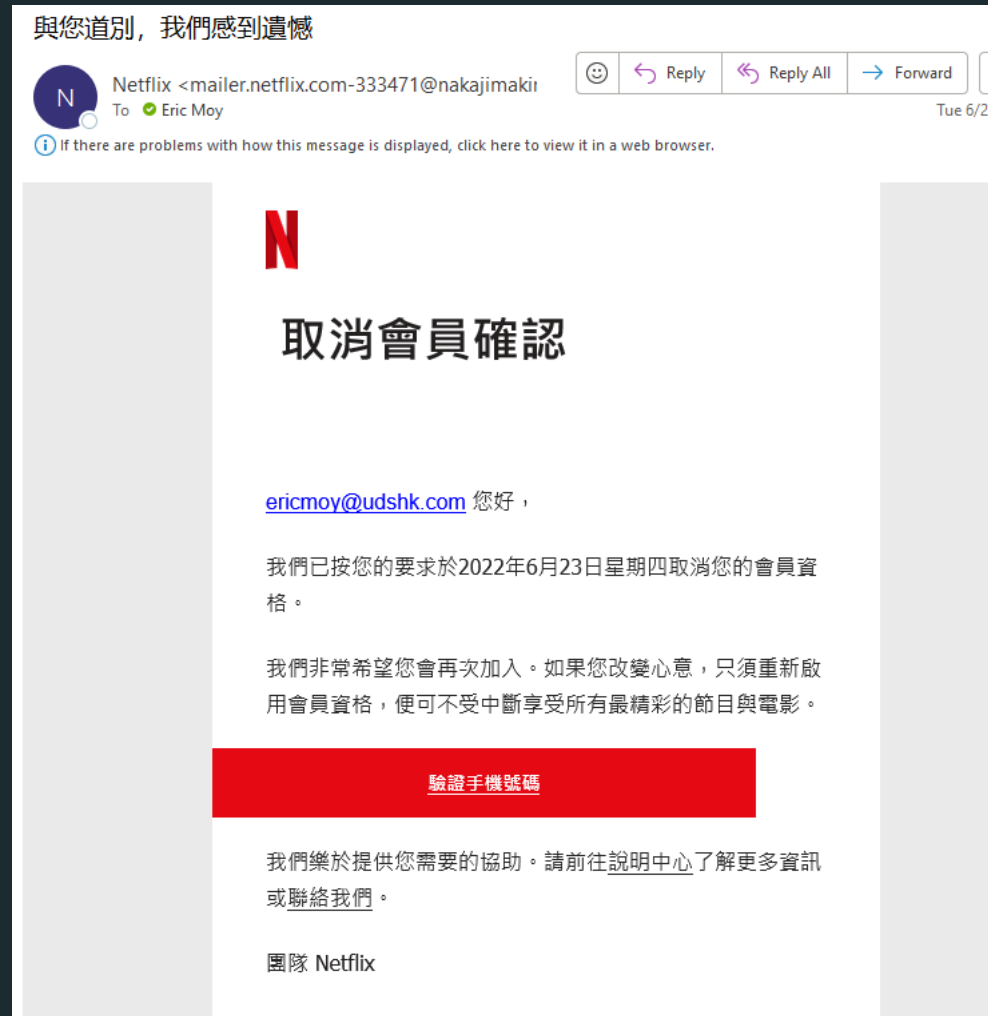


It's essential not to transmit passwords through the same email channel.

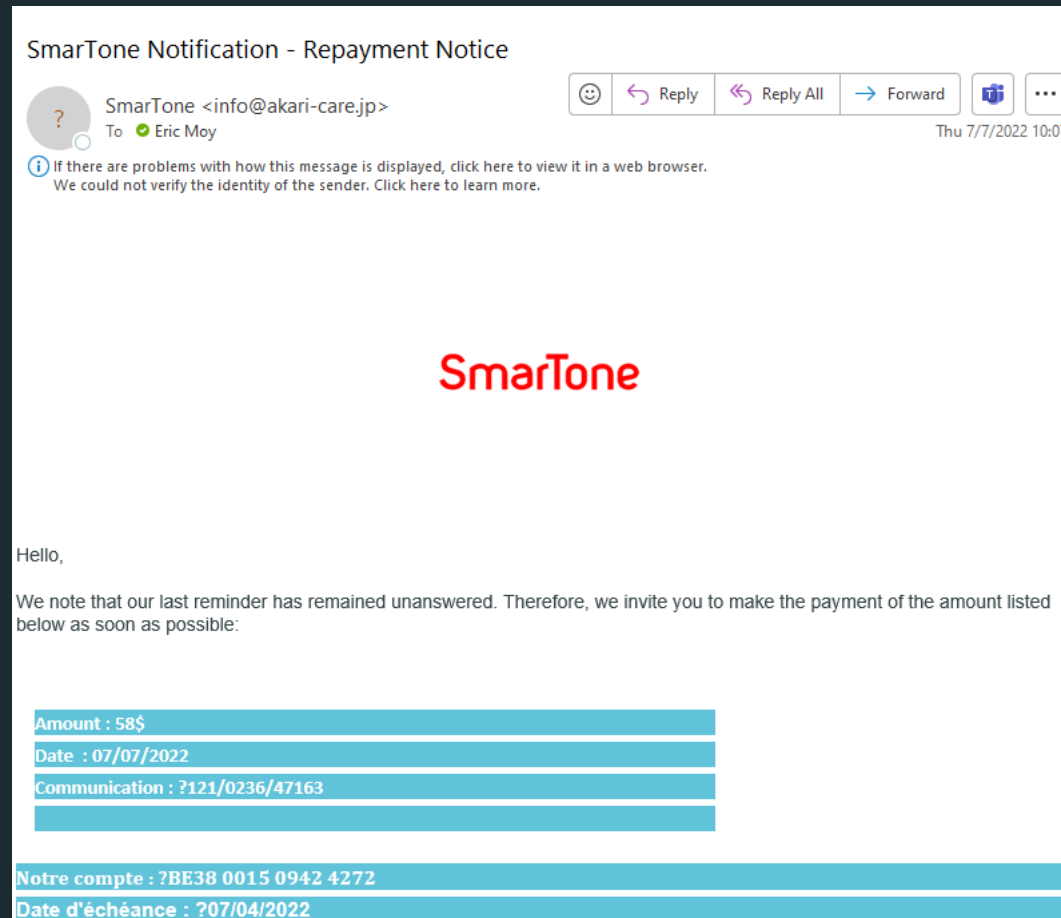
# Phishing example



# Phishing example



# Phishing example





# Phishing example



# Phishing example



# How long does it take this AI to learn to replicate your voice?

Answer: Three seconds

# How to defense AI Crime

- Never share sensitive info with an unverified contact
- Check the URL of each landing page when banking online or using another platform to share sensitive information
- Use strong, unique passwords across all of your accounts

# How to protect yourself against AI voice cloning attack?

- Verify caller Identify
- Establish a unique safe word
- Don't transfer money through unconventional methods
- Use technology safeguards
- Do not speak first to unknown numbers
- Education yourself and others

<https://www.mcafee.com/blogs/internet-security/how-to-protect-yourself-against-ai-voice-cloning-attacks/>

# How to defense AI Crime

- Phishing: Never provide personal financial information, including your Social Security number, account numbers or passwords, over the phone or the Internet if you did not initiate the contact.
- ID theft: Use strong, unique passwords across all of your accounts. Keep your device's security on its strongest setting.
- Deep fakes: Educate yourself and your family: Understanding what deepfakes are and how they can be misused is the first line of defense
- Fake news: Always checking the fact
- Social engineering: Use spam filters to filter emails and messages that seem like phishing attempts or contain spoofed URLs
- Chatbot scams: Use two-factor authentication whenever possible.

# Conclusion

- Individuals feel confident their personal information is safe
- Organizations avoid costly breaches and maintain their reputations
- Regulations are met without issue, avoiding legal complications
- Promoting smoother operations and innovations
- Every individual's data is handled with the highest respect and security
- Organizations seamlessly comply with regulations, building trust and avoiding legal issues
- State-of-the-art encryption and security measures make data breaches nearly impossible
- Everyone knows how their data is being used and stored
- AI systems operate safely and as intended.
- Data privacy seamlessly integrated, with no breaches or leaks.
- Transparent AI operations, fostering trust and accountability.
- Regular updates and rigorous testing, keeping security protocols ahead of emerging threats.

**Data Protection**

**Data Privacy**

**AI Security**





